AO 88 (Rev. 1/94) Subpoena in a Civil Case - SDNY WEB 4/99

Issued by the
UNITED STATES DISTRICT COURT

Northern DISTRICT OF California

UNIVERSAL CITY STUDIOS, INC., et al.,

Plaintiffs,

V.

SHAWN C. REIMERDES, et al.,

Defendants.

SUBPOENA IN A CIVIL CASE

CASE NUMBER: [1] 00 Civ. 0277 (LAK)
(In the Southern District of New York)

TO: Barbara Simons
770 Homer Ave.
Palo Alto, CA 94301

☐ YOU ARE COMMANDED to appear in the United States District Court at the place, date, and time specified below to testify in the above case.

PLACE OF TESTIMONY	COURTROOM
	DATE AND TIME

☒ YOU ARE COMMANDED to appear at the place, date, and time specified below to testify at the taking of a deposition in the above case.

PLACE OF DEPOSITION	DATE AND TIME
United States Courthouse Northern District of California 450 Golden Gate Ave., San Francisco, CA 94102	June 29, 2000 1:00 p.m.

☒ YOU ARE COMMANDED to produce and permit inspection and copying of the following documents or objects at the place, date, and time specified below (list documents or objects):

See schedule A attached.

PLACE	DATE AND TIME
United States Courthouse Northern District of California 450 Golden Gate Ave., San Francisco, CA 94102	June 26, 2000 10:00 a.m.

☐ YOU ARE COMMANDED to permit inspection of the following premises at the date and time specified below.

PREMISES	DATE AND TIME

Any organization not a party to this suit that is subpoenaed for the taking of a deposition shall designate one or more officers, directors, or managing agents, or other persons who consent to testify on its behalf, and may set forth, for each person designated, the matters on which the person will testify. Federal Rules of Civil Procedure, 30(b)(6).

ISSUING OFFICER SIGNATURE AND TITLE (INDICATE IF ATTORNEY FOR PLAINTIFF OR DEFENDANT)	DATE
Attorney for Plaintiffs	June 21, 2000

ISSUING OFFICER'S NAME, ADDRESS AND PHONE NUMBER
William Hart, Esq., (212) 969-3095
Proskauer Rose LLP, 1585 Broadway, New York, New York 10036

(See Rule 45, Federal Rules of Civil Procedure)

[1] If action is pending in district other than district of issuance, state district under case

BAA

PLAINTIFF'S EXHIBIT
40
7-5-00
IGAD-Bayonne, N.J.

SCHEDULE A

DEFINITIONS

A. Southern District of New York Local Civil Rule 26.3 governing Uniform Definitions in Discovery Requests is incorporated herein by reference, and all terms used herein shall be defined as set forth and construed therein, except where otherwise expressly indicated.

B. "**2600**" shall mean the defendant, 2600 Enterprises, Inc. a/k/a "2600 Magazine," its predecessors and successors, its present or former officers, employees, directors, representatives, agents, attorneys and assigns, and its affiliates, subsidiaries, parent or controlling corporations and their affiliates and subsidiaries, or any entity through which it conducts business, either alone or jointly with others.

C. The "**2600.com Site**" shall refer to the web site operated by Defendants at http://www.2600.com, or any other site owned or operated by the Defendants, including all subdirectories and all pages and files presently or previously available for viewing or download at the site.

D. The "**2600 Organizations**" shall refer to any and all organizations of "hackers," other than Defendants, adopting the word "2600" as part of their name.

E. "**2600, The Hacker Quarterly**" shall refer to the print magazine published by Defendants.

F. "**Communicate**," "**communicated**," or "**communication**" means any act or instance of transferring, transmitting, passing, delivering or giving information, in the form of facts, ideas, inquiries, or otherwise, by oral, written, electronic, or any other means.

G. The "**Connecticut Action**" shall refer to the action entitled *Universal City Studios. Inc., et al. v. Hughes*, filed in the United States District Court for the District of Connecticut on January 14, 2000, Case Number 300CV72 RNC.

H. "**Corley**" shall mean the defendant, Eric Corley a/k/a "Emmanuel Goldstein".

I. "**CSS**" shall mean the proprietary copy protection and access control system developed by Matsushita Electric Industrial Co., Ltd. and Toshiba Corporation, known as the Contents Scramble System.

J. "**DeCSS**" shall mean the DVD decryption utility commonly known as DeCSS which has the purpose and function of circumventing CSS or the protection afforded by CSS, and shall include both the compiled object code and source code of DeCSS.

K. "**Defendants**" shall mean Eric Corley a/k/a "Emmanuel Goldstein" ("Corley") and 2600 Enterprises, Inc. a/k/a "2600 Magazine" ("2600"), as defined herein.

L. The term "**document**" is used herein in the broadest possible sense and shall mean any written, graphic or other recorded (whether visually, electronically, magnetically or otherwise) matter of whatever kind or nature or any other means of preserving thought or expression and all tangible things from which information can be processed, transcribed or retrieved, whether originals, copies or drafts (including, without limitation, nonidentical copies), however produced or reproduced (including but not limited to audiotapes, videotapes, CD-ROMs, e-mails, and computer files). A document with handwritten, typewritten or other recorded notes, editing marks, etc., is not and shall not be deemed identical to one without such modifications, additions, or deletions. The term "original" includes the file copy or copies of any document if there is no actual original or

ribbon copy. Designated documents shall mean originals in each instance (or copies thereof if originals are unavailable), regardless of origin or location, which are in your possession, custody, or control, or in the possession, custody, or control of your agents, representatives, employees, or counsel, and any copies or reproductions that differ in any respect from the original, such as copies containing marginal notations or other variations. Designated documents are to be taken as including all attachments, exhibits, enclosures, appendices and other documents that relate to or refer to such designated documents. The enumeration of various specific items as included within the definition of the word "document" shall not be taken to limit the generality of this word, and the requests herein are directed and intended to obtain all "documents" in the broadest and most comprehensive sense and meaning of this word.

M. "**Hyperlink**" shall mean software instructions which, when executed, cause a signal to be sent to another location where data or material can be retrieved for viewing, copying or further transmission.

N. "**Motion Pictures**" shall mean any cinematographic works released on DVD in which Plaintiffs hold a copyright interest.

O. The "**MPAA**" shall mean the Motion Picture Association of America and any of its members, including each of the Plaintiffs.

P. The "**Norway Action**" shall mean any investigation, criminal prosecution or civil action commenced or contemplated by the government of Norway concerning CSS, DeCSS, or any efforts to circumvent the encryption of DVDs.

Q. "**Person**" or "**persons**" shall mean individuals, corporations, proprietorships, partnerships, firms, associations, joint ventures, banks, any government or governmental bodies, commissions, boards or agencies, and all other legal entities, and if appropriate or indicated, divisions, subsidiaries or departments of corporations or other entities, and their principals, agents, representatives, officers or employees.

R. "**Plaintiffs**" shall mean Universal City Studios, Inc.; Paramount Pictures Corporation; Metro-Goldwyn-Mayer Studios Inc.; TriStar Pictures, Inc.; Columbia Pictures Industries, Inc.; Time Warner Entertainment Co., L.P.; Disney Enterprises, Inc.; and Twentieth Century Fox Film Corporation, and shall include their agents, representatives, attorneys, and all persons acting on their behalf.

S. The "**Santa Clara Action**" shall refer to the action entitled *DVD Copy Control Association, Inc. v. McLaughlin, et al.*, filed in the Superior Court of California, Santa Clara County, on December 27, 1999, Case Number CV 786804.

T. The "**Declaration**" shall refer to the Declaration of Barbara Simons In Opposition to Plaintiffs' Motion To Modify the Preliminary Injunction And In Support of Defendants' Cross-Motion To Vacate the Preliminary Injunction, dated April 27, 2000.

INSTRUCTIONS

A. You shall respond to each of the following requests in full to the best of your ability and shall specify which documents and things are responsive to each individual request.

B. Documents shall be provided in the form in which they are normally kept. All documents that consist of or contain information in electronic or digital form, however, shall

be provided on one or more 3.5-inch floppy disks, digital audio tapes ("DATs"), Zip or Jazz cartridges, DVDs, or CD-ROMs unless agreed otherwise.

C. If any responsive document is withheld under a claim of privilege, or for any other reason, you are requested to provide the information set forth in FRCP 26(b)(5) and Southern District of New York Local Rule 26.2 in connection with any such claim.

D. In producing these documents, you are requested to furnish all documents known or available to you, including all documents in your custody or control, or in the custody or control of your officers, directors, agents, employees, representatives, consultants, investigators, or their attorneys or their agents, employees, representatives or investigators.

E. If a document is responsive to a request for production and is in your control, but not in your possession or custody, identify the person with possession or custody.

F. In the event that any document called for by this request has been destroyed or discarded, that document should be identified by (i) any addressor or addressee; (ii) any indicated or blind copies; (iii) the document's date, subject matter, number of pages, and any attachments or appendices, (iv) its date of destruction or discard, and the reason for same; (v) if destroyed or discarded, the persons responsible for carrying out such destruction or discard; and (vi) whether any copies of the document presently exist, and if so, in whose possession.

G. In the event a document is not produced on grounds other than privilege, state the type of document, date, author or addressor, addressee of all copies, recipients of all copies, title, the present location or address of the custodian of all copies, the substance of the content thereof, and state the reasons for its non-production.

H. This request for production shall be deemed continuing, and requires further supplemental production if you receive or discover additional documents after responding to this request.

REQUESTS FOR PRODUCTION

1. All documents within your possession, custody or control concerning DeCSS.

2. All documents reflecting how you first became aware of the existence of DeCSS.

3. All documents concerning your use of DeCSS.

4. All documents concerning any other person's use of DeCSS.

5. All documents concerning the use of DeCSS by any person for purposes other than to decrypt a DVD, including but not limited to, any documents concerning the use of DeCSS for research, study or reverse-engineering.

6. All documents concerning internet locations where DeCSS is, or was, available.

7. All documents concerning communications relating to internet locations where DeCSS is, or was, available.

8. All documents concerning any efforts to encourage or solicit any person to make DeCSS available on the internet.

9. All documents concerning communications sent to, or received from, any person concerning the MPAA, CSS, DeCSS, this litigation, the Connecticut Action, the Santa Clara Action, or the Norway Action, including but not limited to e-mail communications and archived discussions in "chat rooms" or any other electronic forum.

10. All documents concerning the Declaration, including all drafts of the Declaration, all notes and correspondence relating to the Declaration, and all documents reviewed in connection with its preparation.

11. All documents concerning, demonstrating, supporting, or detracting from, any statement in the Declaration.

12. All documents concerning communications between or among you and any parties to this action, including but not limited to, communications with defendants' counsel.

13. All documents concerning communications between or among you and any owners, employees, agents, parents, subsidiaries, and/or other individuals associated with the 2600 Organizations, concerning the MPAA, CSS, DeCSS, this litigation, the Connecticut Action, the Santa Clara Action, or the Norway Action.

14. All documents that you may rely on if you are called as a witness at trial in this action.

15. All documents reviewed in preparation for your deposition in this action.

16. All documents concerning encryption, security or other access- or copy-control systems that have been hacked, cracked or reverse-engineered.

17. All documents reflecting communications concerning encryption, security or other access- or copy-control systems that have been hacked, cracked or reverse-engineered.

18. A list of all publications that you authored in the past ten years.

19. Copies of all publications that you authored relating to any statements in the Declaration, or otherwise relating to this action.

20. All documents concerning compensation that you received or will receive in connection with this action, including, but not limited to, compensation for the preparation of the Declaration or for appearing at a deposition or trial.

21. A list of all other legal proceedings in which you have testified as an expert at trial or by deposition.

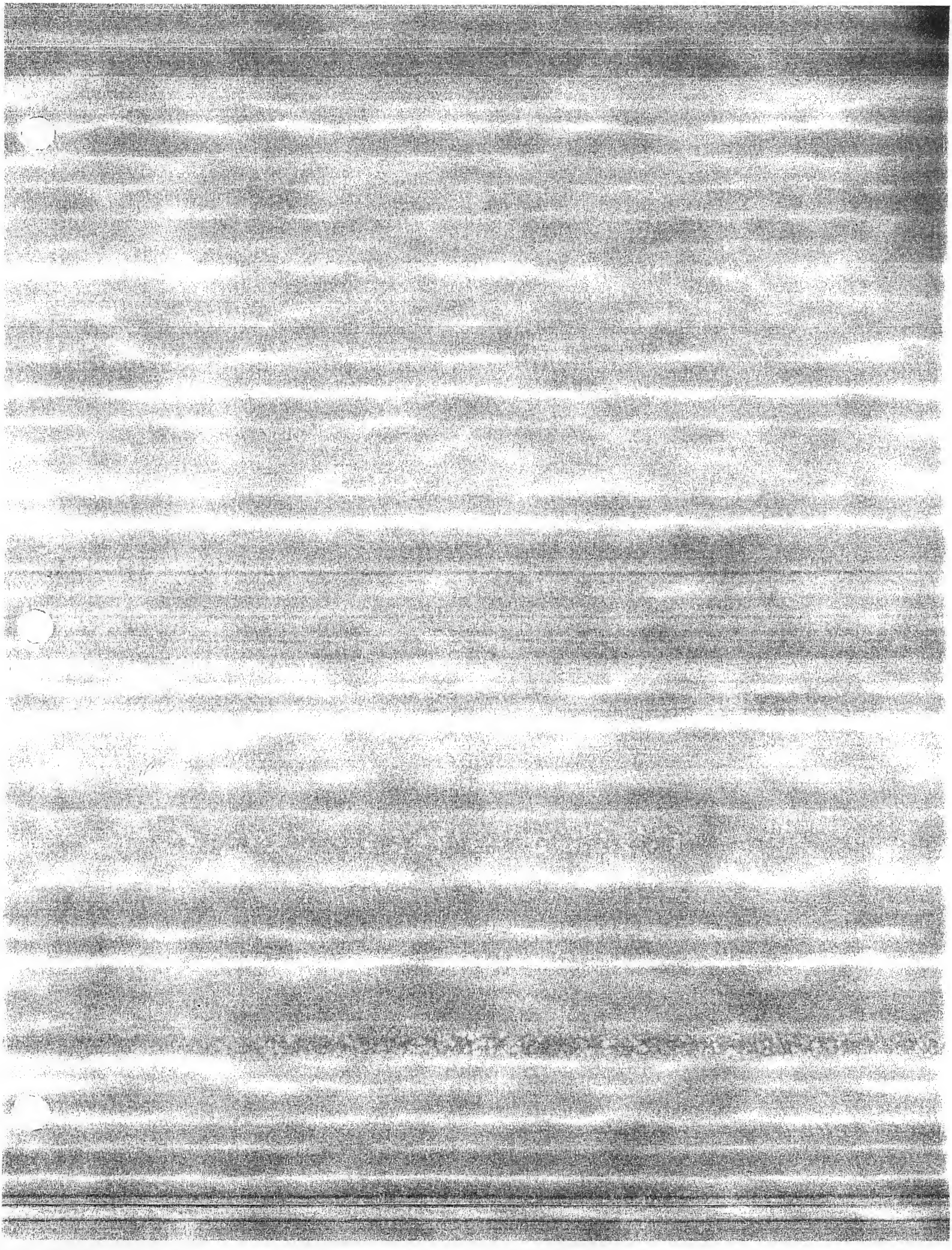
22. All documents concerning any incidents in which you have been accused of violating any person's intellectual property rights.

23. All documents concerning technology for the compression of video signals.

24. All documents concerning statements you have made to the press or media relating to copyrights, intellectual property rights, or free access to copyrighted materials, including, but not limited to, all reports, articles and publications containing your statements on these subjects.

25. All documents concerning the feasibility of transmitting video on the internet.

26. All documents concerning the trafficking or feasibility of trafficking of movies on the internet.



Martin Garbus, Esq. (MG 6261)
Edward Hernstadt, Esq. (EH 9569)
FRANKFURT, GARBUS, KLEIN & SELZ, P.C.
488 Madison Avenue
New York, New York 10022
(212) 826-5582

Attorneys for Defendant Eric Corley a/k/a
EMMANUEL GOLDSTEIN

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

UNIVERSAL CITY STUDIOS, INC., PARAMOUNT PICTURES CORPORATION,. METRO-GOLDWYN-MAYER STUDIOS INC., TRISTAR PICTURES, INC., COLUMBIA PICTURES INDUSTRIES, INC., TIME WARNER ENTERTAINMENT CO., L.P., DISNEY ENTERPRISES, INC., and TWENTIETH CENTURY FOX FILM CORPORATION,

Plaintiffs,

- against -

SHAWN C. REIMERDES, ERIC CORLEY a/k/a "EMMANUEL GOLDSTEIN" and ROMAN KAZAN,

Defendants

00 Civ. 0277 (LAK)

DECLARATION OF BARBARA SIMONS IN OPPOSITION TO PLAINTIFFS' MOTION TO MODIFY THE PRELIMINARY INJUNCTION AND IN SUPPORT OF DEFENDANTS' CROSS-MOTION TO VACATE THE PRELIMINARY INJUNCTION

----------X

I, BARBARA SIMONS, declare under penalty of perjury that the foregoing is true and correct:

1. I am presently the President of the Association for Computing Machinery ("ACM"), a position I was elected to hold in 1998. ACM is the oldest educational and technical computer society in the world, with about 80,000 members internationally. Prior to becoming

PLAINTIFF'S EXHIBIT 2 Simons 7-6-00
PENGAD-Bayonne, N. J.

president, I chaired ACM's U.S. Technology Policy Committee (USACM), which I also founded. As President of the ACM, I submitted comments regarding the anti-circumvention provisions of Section 1201(a) of the "Digital Millenium" amendment to the Copyright Act ("Section 1201"). A copy of this letter is attached hereto as Exhibit A, and can be found at: http://www.acm.org/usacm/copyright/dmca.exemption.htm. I was also one of eight presidents of professional societies -- the American Association for the Advancement of Science, American Association of Artificial Intelligence, American Mathematical Society, American Statistical Association, Association for Computing Machinery, Computer Research Association Society for Industrial and Applied Mathematics, and The Institute of Electrical and Electronics Engineers-USA — who signed a letter regarding the Section 1201 to Senator Orrin Hatch in September 1998. A copy of that letter is attached hereto as Exhibit B and can be found at: http://www.acm.org/usacm/copyright/presidents-letter-998.html

2. Prior to being elected President of ACM in 1998, I chaired ACM's U.S. Technology Policy Committee (USACM) and the ACM Committee for Scientific Freedom and Human Rights. I was elected Secretary of the Council of Scientific Society Presidents (CSSP) in 1999, and have been on the CSSP Board since 1998. I have also been a member of the U.C. Berkeley Engineering Fund Board of Directors since 1998. I am a Fellow of ACM and of the American Association for the Advancement of Science.

3. I earned my Ph.D. in computer science from U.C. Berkeley; my dissertation solved a major open problem in scheduling theory. I became a Research Staff Member at IBM's San Jose Research Center (now Almaden), where I did research on scheduling theory, compiler optimization, and fault tolerant distributed computing, and received an IBM Research Division Award for my work on clock synchronization. I then joined IBM's Applications Development

Technology Institute and subsequently served as senior technology advisor for IBM Global Services. I hold several patents and have authored numerous technical papers.

4. The University of California, Berkeley will present me with the Distinguished Alumnus Award in Computer Sciences and Engineering in May 2000. I was selected by c|net as one of its 26 Internet "Visionaries" and was named one of the "Top 100 Women in Computing" by Open Computing. I have received the Norbert Wiener Award from the Computer Professionals for Social Responsibility, and the Pioneer Award from the Electronic Frontier Foundation; Science Magazine featured me in a special edition on women in science in 1992.

5. Currently, I serve on the President's Export Council's Subcommittee on Encryption, and I have been a member of the Information Technology Working Group of the President's Council on the Year 2000 Conversion. I have testified before both the U.S. and the California legislatures and at government sponsored hearings on cryptography, medical privacy, authentication for access to on-line records, and intellectual property on the Internet. My complete Curriculum Vitae is attached hereto as Exhibit C.

6. I make this declaration because I believe that the right to post and conduct discussions about DeCSS (an application which can be used to decrypt Content Scrambling System ("CSS"), the encryption software for DVD movie disks) and similar "security systems" for copyrighted materials is very important to the entire academic and scientific enterprise. Participants in this enterprise, including academics, scientists, professionals, hobbyists, amateurs and more, rely on the freedom to exchange information. Over the past years, the Internet has become an increasingly important medium for the exchange of ideas and information, providing interested parties with access to thousands of different web sites publishing a multitude of ideas and speech. Many web sites address matters of concern to the academic and scientific enterprise

and provide an easily accessible, widely available forum for the exchange of ideas. I believe that freedom of speech on the Internet is crucial to this enterprise, including speech such as the DeCSS source code.

7. Freedom to speak without restraint is especially vital to research and development projects. For example, I understand that there are on-going development projects that were undertaken in order to build a DVD player to play legally purchased DVDs on open-source operating systems (such as Linux).

8. I do not believe that posting or linking to DeCSS poses any real threat of illegal commercial copying, or of the distribution of modes for copying DVDs. The primary commercially relevant purpose for DeCSS of which I am aware is as a useful tool (itself reverse engineered) to use on the larger reverse engineering project of building a universal DVD player.

9. The current legal DVD battle between the movie industry and the free/open software communities over DVD is a microcosm of an ongoing dispute about intellectual property generally. This dispute pits intellectual property owners against such diverse groups as programmers opposing restrictions on reverse engineering and the publication of computer code and librarians opposing new restrictions on copyright rights of first sale and fair use.

10. One of the reasons that the myth of a Norwegian teenager's breaking CSS took hold is that CSS is amazingly weak. CSS uses only a 40-bit key, a length known to be breakable in a few minutes. It also employs a proprietary algorithm, rather than one that has been extensively tested in the public domain. The copy protection system relies heavily on obfuscation which, together with the carelessness of at least one licensee, appears to have created additional opportunities to break the system. Another reason was the reaction of the online community. I have been informed that a large number of Internet citizens downloaded DeCSS

during the first week it was posted (many, I believe, in order to have it if the source code was ever enjoined). The reaction to the arrest of the Norwegian teenager who originally posted DeCSS and the lawsuits filed by the DVD CCA and MPAA was equally immediate, and led to thousands more people downloading DeCSS and/or creating mirror sites of the program.

11. Foreknowledge of and concerns about the vulnerability of this protection scheme appears to have been a motivating factor for extensive lobbying by Hollywood and the DVD manufacturers on behalf of the anti-circumvention component of Section 1201. There have been reports that the Film Industry, working in concert with computer and consumer electronic companies, arrived at a unique solution: it submitted strict Anti-Circumvention legislation to Congress in the hopes of having Congress pass a law to criminalize products or actions that would bypass the copy protection system.

12. The DVD Copy Control Association (DVD CCA) was created in December, 1999 — that is, several months after DeCSS was developed and it was first posted it on the Internet -- to issue licenses. I have been informed, and it is my understanding, that to obtain a license, one pays a fee and signs an agreement pledging not to produce non-compliant machines or to reveal the copy protection scheme. The Linux community was divided: CSS had to be dealt with if a Linux DVD player were to be developed, but how to handle the licensing issues? One group, LSDVD, has been working on a licensed DVD player; another, LiViD, is working on creating a free open source version of DVD for Linux.

13. This case was brought by the eight largest movie studios based on the Section 1201. In the California case, the plaintiff DVD CCA filed a copy of the DeCSS source code it has claimed in that case is a trade secret. Although the Court file of the now-notorious "Hoy Declaration" has since been sealed, a number of people reviewed it and posted it on the Internet

(for example, at http://cryptome.org/dvd-hoy-reply.htm#Exhibit). It's even available on a T-shirt (at http://copyleft.net/cgi- in/copyleft/t039.pl?1&back)!

14. I am informed that many of those involved with breaking CSS say they did so to make it possible to play DVDs on Linux and other free/open-source based operating systems, and I am aware that such projects are currently underway. Although the plaintiffs in this case appear to believe that the Section 1201 prohibits almost all reverse engineering of copy-protection systems, that is not the case. For example, reverse engineering for interoperability is specifically exempted from the Section 1201's anti-circumvention provisions. I believe that this exemption would directly apply to the use (or publication) of DeCSS as a step in or part of a project to build a DVD player for use on the Linux and/or other open-source platforms.

15. The plaintiffs in this and the California action have never accused anyone of using DeCSS to make illegal copies of DVDs. However, the latest motion filed by the New York plaintiffs seeks to prohibit the New York defendants' providing hyperlinks to web sites from which DeCSS could be downloaded. Barring hyperlinks is a frightening prospect. I believe that if this Court were to prohibit the defendants from linking to web sites that post DeCSS, not only would it restrain an extraordinary amount of speech in addition to the DeCSS source code, but it would have no impact on the copying the MPAA claims will surely follow from DeCSS: all of the linked-to web sites with DeCSS will still be on the Internet. In this regard, I will note that DeCSS is not a prerequisite for making illegal copies, since other CSS descramblers exist and are available on the Internet. Further, I do not believe that CSS was primarily intended to prevent illegal copying of DVDs for commercial purposes: given the weaknesses of the DVD copy protection system, it was, as the DVD CCA was aware, only a matter of time before CCS would be broken.

16. I am personally familiar with problems related to the ease of copying digitized material in connection with the Association for Computing Machinery's digital library, which is financially successful even though our copyright policy allows unlimited non-commercial copying. I do not claim that the proportionally smaller scale model of a not-for-profit professional society is directly applicable to the DVD industry. However, given that experience, and the fact that, to the best of my knowledge, the industry has historically made a number of claims about copying that are unsupported by objective studies, I believe the Movie Industry's present claims that their survival depends upon a reading of the Section 1201 that would prohibit any access to the copyrighted work in its digital DVD format, even by the consumer who purchased it, is unsupported.

17. Our scientific and technological success as a nation has relied heavily on the "fair use" of copyrighted materials. For this reason, and because of our interest in and concern about education, ACM has strongly supported consumers' rights under the Copyright Act, and in particular, the fair use right. It is clear to me that if such rights are not preserved, if the plaintiffs in this case are permitted to use Section 1201 to ban any utility that negates CSS and permits noninfringing access to copyrighted works, essential rights such as fair use will be limited to a small technological elite. If such utilities are not generally available, then only persons technologically skilled enough to create the requisite tool will be able to exercise their fair use rights; the rest of the world will not. That cannot be the intention of Section 1201.

Dated: April 27, 2000
Palo Alto, California

EXHIBIT A

Comments to the Copyright Office of the Library of Commerce

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies

February 17, 2000

Pursuant to the "Request for Comments on Section 1201(a) of the Digital Millennium Copyright Act," the Association for Computing Machinery urges you to criminalize only those who circumvent technological protection mechanisms with the intent to infringe. The legislation must be revised to ensure the freedom of scientists to bypass copy protection schemes for fair use purposes. Scientists must be legally permitted to circumvent access technologies in order to recognize shortcomings in security systems. Prohibitions on such legitimate behaviors would undermine efforts to create a robust system that can endure rigorous scrutiny.

The Association for Computing Machinery is a leading society of computer scientists in education, industry, and government. ACM facilitates communication between computer professionals and policymakers on issues of concern to the computing community.

The Digital Millennium Copyright Act must expressly allow the use of circumvention measures for fair use purposes. The fair use doctrine is fundamental to copyright law, which is derived from the U.S. Constitution and underscores the necessity "to promote the Progress of Science and the useful Arts" (U.S. Constitution, Article 1, 8). The draconian criminal measures imposed for violation of section 1201 will deter individuals from conducting bona fide forms of science and technology research that is fundamental to innovation. A recent high-profile case in the media pertains to the discovery of the weak encryption algorithm of the copy-protection system of DVDs. Scientists must be legally permitted to circumvent access technologies in order to recognize shortcomings in security systems. Critical to the scientific endeavor is the freedom to explore, to understand, and to assess. It is simply inappropriate for the government to attempt to regulate basic research techniques.

The anti-circumvention provision of the Act criminalizes research that is necessary for computer and network security. Although the bill sets out exceptions on encryption research, the majority of computer security research does not involve encryption. Even the exceptions for encryption are limited and will not cover sufficiently a wide range of computer research. Computer security researchers believe that not only will their research be prohibited, but even the teaching of many of the standard security techniques will constitute a crime. As a consequence, experts in computer security may not be able to take the steps necessary to safeguard the nation's computer systems.

The exceptions in the DMCA to permit the circumvention of technological protection mechanisms are overly narrow and restrictive, and many legitimate noninfringing uses are ignored. For example, a firm might want to test a computer system before purchasing it to ensure that it is trustworthy and secure. The Act allows computer security testing only by the owner or operator of a system, so the firm would be able to test the robustness of the system only with the producer's permission. In another case, a copyright owner might suspect that another Internet user is infringing his work. The only way to test his assumptions would be to bypass the encryption scheme of the suspected work to assess the material. Amendments to the legislation should distinguish between infringing and noninfringing uses and assign liability only to those who use circumvention technology with the intent to infringe.

A further problem is that anti-circumvention exemptions become meaningless if access mechanisms are not allowed. The Act provides an exemption for nonprofit libraries, archives, and educational institutions permitting them to circumvent copy-protection schemes to obtain authorized access to a work, yet the

Act bans equipment and services designed to enable circumvention. A prohibition of the manufacture, import, and use of tools necessary to enable circumvention essentially annuls any effective means to obtain access to a work for a legitimate use.

We urge you to recognize the distinction between circumvention for the purpose of obtaining unauthorized access to a work and circumvention for the purpose of making a non-infringing use of a work. Absent some clear criminal intent, scientists should not be penalized for conducting research that is crucial to developing and testing copyright protection systems. The ability of computer scientists to engage in critical research and to exchange ideas and information that enable innovation are fundamental to science. Thank you for this opportunity to offer our comments. Please contact us with additional questions.

Respectfully submitted,

Dr. Barbara Simons, President
Association for Computing Machinery

EXHIBIT B

AAAS • AAAI • AMS • ASA • ACM • CRA • SIAM • IEEE

September 14, 1998

Senator Orrin G. Hatch
Chairman
Senate Judiciary Committee
224 Dirksen Building
Washington, D.C. 20510

Dear Chairman Hatch,

As presidents of leading U.S. science and engineering societies, we are writing to you regarding H.R. 2281, the Digital Millennium Copyright Act. We are particularly concerned that the database and the anti-circumvention provisions of the Act will have substantial negative impacts on the conduct of basic research. They also will slow the progress of important technology developments, and reduce beneficial economic returns of research and development to society. Indeed, several of the undersigned organizations have submitted specific legislative proposals to improve H.R. 2281.

The science and technical communities are dependent on the fair use privilege for research, teaching, and development. They traditionally have made data and information derived from publicly funded research available with minimal restrictions and for no more than the cost of reproduction and dissemination. Unfortunately, the fair use provision in Title V of H.R. 2281, the section that applies to databases, will create many obstacles for our communities.

Databases that are time dependent, such as telescope readings, are impossible to replicate. Others, such as the human genome sequence data, are costly and impractical to duplicate. There is even concern that the "potential uses" restriction could prohibit the use of statistical or other analytic techniques on protected data, especially if a resulting statistical product has commercial value. Such a prohibition could seriously damage U.S. science, engineering, and financial analysis, as well as data product innovation.

On July 10, 1998, the presidents of the three national academies sent the enclosed letter in which they express "serious concern" about the proposed legislation. Many of the reasons for their concern remain in Title V. Any legislation that does not retain the traditional fair use privileges under which scientists always have operated will have a chilling effect on science.

The proposed database provisions also could harm U.S. industry. Quoting from "Bits of Power," a report issued by the National Research Council in 1997:

> "... [S]uch an approach ignores the contribution of basic science to the ability of U.S. firms to predominate in markets for technology and information goods. Despite a general consensus on the need for sustained levels of investment in research and development, the proposed database laws could change the status quo without anyone's wanting it to happen by elevating the price of the one raw material to which U.S. researchers have always had ready access. If less available scientific information were to translate to fewer applications of economic importance, the end result would be a loss of U.S. technological competitiveness in an integrated world market."

While we understand the desire to protect investments made in large data collections, the proposed legislation fails to recognize the legitimate needs of academic, professional, scientific, and ordinary users of data.

A second major flaw in H.R. 2281 involves the anti-circumvention provisions. Since many of the techniques that are used to break into systems are also used to test system security, the legislation would outlaw devices and technologies that are crucial for making information processing systems trustworthy and secure. By attempting to regulate technologies rather than infringing behavior, progress of research

in cryptography and other computer security areas could be significantly hindered.

Although the bill includes limited exceptions on circumvention (Title I Sec. 1203) for encryption research, the majority of computer security research does not involve encryption. Leading computer security researchers fear that the legislation may criminalize not only their research, but even the teaching of many of the standard security techniques. (See the enclosed letter.) Similarly, the bill's exemption to permit reverse engineering for the sole purpose of interoperability may criminalize development of software engineering tools and technology with other uses, such as fixing Year 2000 problems in software. The consequences are potentially catastrophic.

A bill with sections entitled "Permissible Acts of Encryption Research" or even "Permissible Acts of Security Research" is too cumbersome for the scientific research community. Scientists should not be required to consult lawyers to determine if their previously legitimate research might be in violation of the law. Furthermore, because it is impossible to anticipate the direction and nature of all research, the approach of exempting scientific research is fundamentally flawed.

We believe that H.R. 2281 would prohibit bona fide forms of science and technology research that benefit us all, and we urge you to reconsider the approach used in H.R. 2281. We would welcome the opportunity to work with you on a version of the bill that preserves the freedom of American scientific research and does not threaten our long term economic security.

Sincerely,

Dr. M.R.C. Greenwood, President,
American Association for the Advancement of Science

Dr. David L. Waltz, President,
American Association of Artificial Intelligence

Dr. Arthur Jaffe, President,
American Mathematical Society

Dr. David S. Moore, President,
American Statistical Association

Dr. Barbara Simons, President,
Association for Computing Machinery

Dr. Ed Lazowska, President,
Computer Research Association

Dr. John Guckenheimer, President,
Society for Industrial and Applied Mathematics

Dr. John R. Reinert, President,
The Institute of Electrical and Electronics Engineers-USA

cc: Senate Judiciary Committee
Senate Commerce Committee
Senate Majority Leader Trent Lott
Senate Minority Leader Thomas Daschle

EXHIBIT C

Curriculum Vitae

Barbara Simons
770 Homer Ave.
Palo Alto CA, 94301
650.328.8730 voice / 650.617.3709 fax
simons@acm.org

Education

Ph.D. in computer science from the University of California, Berkeley, in June 1981 - thesis advisor Richard Karp. My dissertation, *Scheduling with Release Times and Deadlines*, solved a major open problem in scheduling by developing the first known algorithm for the problem.

Employment

- Senior Technology Advisor, IBM Global Services, IBM Corp., Nov. 1996 - Jan. 1998; worked with IBM researchers and business people to develop and provide research solutions to business problems.
- Researcher, Application Development Technology Institute, IBM Corp., Oct. 1992 - Nov. 1996; research on compiler optimization problems and development of a prototype backend for retargeting optimized code.
- Research, Foundations of Computer Science Group, IBM Research, Jan. 1980 - Sept. 1992; research areas included scheduling theory, fault tolerant computing, compiler optimization, and communicating sequential processes.
- Professor, U.C. Santa Cruz, Sept. 1984 - Dec. 1984; taught the graduate algorithms course.

Honors

- Distinguished Alumnus Award in Computer Sciences and Engineering, U.C. Berkeley, May 21, 2000.
- ACM President, 1998 - 2000.
- EFF Pioneer Award 1998.
- Selected as one of 26 Internet "Visionaries" by c|net, Dec. 1995.
- Selected as one of the Top 100 Women in Computing by Open Computing, Dec. 1994.
- Fellow, Association for Computing Machinery (ACM), elected 1993.
- Fellow, American Association for the Advancement of Science (AAAS), elected 1993.
- Featured in special issue of *Science* on Women in Science, 1992.
- CPSR Norbert Wiener Award for Professional and Social Responsibility in Computing, 1992.
- IBM Research Division Award for work on clock synchronization, 1988.

Patents

- Retargeting Optimized Code by Matching Tree Patterns in Directed Acyclic Graphs, with Vivek Sarkar and Mauricio Serrano, patent pending.
- A Method of, System for, and Computer Program Product for Providing Efficient Utilization of Memory Hierarchy through Code Restructuring, with Dz Ching Ju, K. Muthukumar, and Shankar Ramaswamy, patent pending.
- A System, Method, and Program Product for Loop Instruction Scheduling for Hardware Lookahead, with Vivek Sarkar, patent pending.
- A System, Method, and Program Product for Instruction Scheduling in the Presence of Hardware Lookahead Accomplished by the Rescheduling of Idle Slots (Patent number 5887174), with Vivek Sarkar.
- Decentralized Synchronization of Clocks (Patent numbers 4584643 and 4531185), with Danny Dolev, Joe Halpern, and Ray Strong

Publications

- To DVD or not to DVD, *Commun. ACM* 43, 5, May 2000, pp. 31-32.
- Trademarking the Net, *Commun. ACM* 43, 1, March 2000, pp. 27-28.
- Not Now, Not Like this: Why the ACM Council Does not support the licensing of software engineering at this time, with Fran Allen and Paula Hawthorn, *Commun. ACM* 43, 1, Jan. 2000, pp. 29-30.
- Building Big Brother, *Commun. ACM* 43, 1, Jan. 2000, pp. 31-32. Also, in *iMP* (an on-line publication), February 2000.
- The Heroes Among Us, *Commun. ACM* 42, 10, Oct. 1999, pp. 25, 112. Also, in *iMP*, March 2000.
- Melissa's Message, *Commun. ACM* 42, 6, June 1999, pp. 25-26.
- Regulating Content on the Internet, a chapter in *Capital for Our Time*, Hoover Institution Press, Stanford, CA, 1999, pp. 156-174.
- Starr Wars, *Commun. ACM* 42, 1, Jan. 1999, pp. 26-27.
- Outlawing Technology, *Commun. ACM* 41, 10, Oct. 1998, pp. 17-18.
- Optimizations for Efficient Array Redistribution on Distributed Memory Multiprocessors, with Shankar Ramaswamy and Privthviraj Banerjee, *Journal of Parallel and Distributed Computing*, 1996, 38, 1996, pp. 217-226.
- Anticipatory Instruction Scheduling, with Vivek Sarkar, *8th Annual ACM Symposium on Parallel Algorithms and Architecture* (SPAA 96), Padua, Italy, June 24-26, 1996, pp. 119-130.
- Dynamic Fault-Tolerant Clock Synchronization, with Danny Dolev, Joseph Halpern, and Ray Strong, *Journal of the ACM* 42:1, 1995, pp. 143-185.
- Static Analysis of Interprocess Communication, with Peter Ladkin, *Responsive Computer Systems: Steps Toward Fault-Tolerant Real-Time Systems*, ed. D. Fussell and M. Malek, Kluwer Academic Publishers, 1995.
- An Optimal Scheduling Algorithm for Instruction Lookahead, with Vivek Sarkar, the *IBM Programming Technology Forum* (IBM Confidential), Research Triangle Park, NC, June 5-6, 1995, pp. 125-137.
- Questions Concerning the NII, *Computer Related Risks*, by Peter Neumann, published by ACM Press, 1995, pp. 302-304.
- Constructing a Control Flow Graph for Parallel Code, IBM TR ADTI-1995-003 or STL TR 3.606, Dec. 1994. Accepted for publication in *Transactions on Programming Languages* (TOPLAS).
- A Fast Heuristic for Loop Parallelization, with Richard Anderson, a special issue of *Parallel Processing Letters*, 4(3), 1994, pp. 281-299.
- Static Analysis of Multiway Synchronization, with Peter Ladkin, *Proceedings of the fourth annual IBM Centre for Advanced Studies Conference* (CASCON'94), Toronto, Canada, Oct. 31 - Nov. 3, 1994, pp. 142-156.
- Code Positioning for Procedures and Basic Blocks, IBM Technical Report ADTI-1994-006, Oct. 1994.
- Compiler Solutions to False Sharing Elimination, with Jyh-Herng Chow and Vivek Sarkar, *Proceedings of the IBM Programming Technology Forum* (IBM Confidential) Yorktown Heights, NY, June 6-7, 1994, pp. 259-276.
- Parallel Program Graphs and their Classification, with Vivek Sarkar, Proceedings of the Sixth Annual Languages and Compilers for Parallelism Workshop, Portland, Oregon, Aug. 12-14, 1993. Springer-Verlag *Lecture Notes in Computer Science*, Vol. 768, Jan. 1994, pp. 633-655.
- Compiler Solutions for the Stale-Data and False-Sharing Problems, with Mauricio Breternitz, Michael Lai, and Vivek Sarkar. *Proceedings of the Programming Languages Technology ITL Meeting*, June 8 - 9, 1993, Rochester, Minn., pp. 5-1 - 5-23, IBM confidential. Also in *Proceedings of the 27th Hawaii International Conference on System Sciences*, Maui, Hawaii, Jan. 4-7, 1994.
- Scheduling Time-Critical Instructions on RISC Machines, with Krishna Palem, *Transactions on Programming Languages* (TOPLAS), 15, No. 4, 1993, pp. 632-658. Also appeared in 17th Annual ACM Symposium on Principles of Programming Languages (POPL), San Francisco, CA, Jan. 17-19, 1990, pp. 270-280.
- Deadlock Detection for CSP-type Communications, with Peter Ladkin, *Proceedings of the Third International Workshop on Responsive Computer Systems*, Sept. 29 - Oct. 1, 1993, Lincoln, New Hampshire, pp. 229-239; a chapter in *Responsive Computer Systems: Steps Toward Fault-Tolerant Real-Time Systems*, ed. D. Fussell and M. Malek, Kluwer Academic Publishers, 1995.

- An Efficient Algorithm for Constructing a Control Flow Graph for Parallel Code, with Jeanne Ferrante, IBM Technical Report TR 03.465-1, Feb. 1993.
- Simple NP-Complete Deadlock and Reachability Problems, with Peter Ladkin, IBM Technical Report TR.03.456, Nov. 1992.
- Compile-Time Analysis of Communicating Processes, with Peter Ladkin, *Proc. ACM 1992 International Conference on Supercomputing*, Washington, D.C., July 19-23, 1992, pp. 248-259.
- Static Analysis of Concurrent Communicating Loops, with Peter Ladkin, IBM Research Report RJ 8625, Feb. 1992. The report is a revision of RJ 8062 with P. Ladkin entitled "Two Combinatorial Conditions for Statically Analyzing Concurrent Communicating Loops". An early version of this work, "Analyzing Communicating Processes," appeared in the *Proceedings of the 1990 IBM Programming Languages ITL*.
- Instruction Scheduling for Compilers, with Krishna Palem, IBM Research Report 8535, Dec., 1991. Written to appear as a chapter in *Optimization in Compilers*, edited by Fran Allen, Barry Rosen, and Kenny Zadeck.
- On Building a Research Agenda for Computer Science, *The Communications of the ACM*, 34, No. 10, Oct. 1991, pp. 121-125.
- Generating the Flow Graph for Communicating Parallel Loop Processes, with Peter Ladkin, IBM Research Report RJ 8093, April 1991.
- Coalition for Science and Technology, *ACM MemberNet*, Jan. 1991, pp. 1 and 8.
- *Fault Tolerant Distributed Computing*, coedited with Alfred Spector, Springer-Verlag Lecture Notes in Computer Science, Vol. 448, New York, 1990.
- Scheduling Sequential Loops on Parallel Processors, with Ashfaq Munshi, *SIAM J. on Comput.*, 19, No. 4, 1990, pp. 728-741.
- A Foundation for Sequentializing Parallel Code, with David Alpern and Jeanne Ferrante, *Proc. 2nd ACM Symposium on Parallel Algorithms and Architectures*, Crete, Greece, July 2-6, 1990.
- A Fast Algorithm for Multiprocessor Scheduling of Unit-Length Jobs, with Manfred Warmuth, *SIAM J. on Comput.*, 18, No. 4, 1989, pp. 690-710.
- Parallelism, Compiler Optimization, and Deterministic Scheduling Theory, A position paper, *Proc. Opportunities & Constraints of Parallel Processing*, San Jose, CA., Dec. 5-6, 1988.
- On Pipeline Scheduling with Deadlines, with Krishna Palem, IBM Research Report RJ 6592, 1988, San Jose, Ca.
- An Overview of Clock Synchronization, with J. Lundelius and N. Lynch, a chapter in *Fault Tolerant Distributed Computing*, edited by Barbara Simons and Alfred Spector, Springer-Verlag, New York, Oct 1990.
- Computing the Bump Number of a Partial Order with Techniques from Two-Processor Scheduling, with Alexandro A. Schaffer, *Order*, 5, 1988, pp. 131-141.
- Generating Sequential Code from Parallel Code, with Jeanne Ferrante and Mary Mace, *Proc. ACM 1988 International Conference on Supercomputing*, St. Malo, France, July 4-7, 1988, pp. 582-592.
- A scheduling Problem Arising from Loop Parallelization on MIMD Machines, with Richard Anderson and Ash Munshi. *VLSI Algorithms and Architectures*, Springer-Verlag Lecture Notes in Computer Science, June/July, 1988, pp. 124-33.
- Federal Funding in Computer Science: a Preliminary Report, with Joel Yudken, IBM Research Report RJ 6235, 1988, San Jose, Ca.
- A New Look at Fault Tolerant Network Routings, with D. Dolev, Joseph Halpern, and Ray Strong, *Information and Computation*, 72, 1987, pp. 180-196.
- Efficient Fault Tolerant Routings in Networks, with Andrei Broder, Danny Dolev, and Michael Fischer, *Information and Computation*, 75, 1987, pp. 52-64.
- On Placing Tiles in the Plane, with Andrei Broder, *Foundations of Data Organization*, eds. S. Ghosh, Y. Kambayashi, and K. Tanaka, Plenum Press, 1987, pp. 207-233.
- On Fault Tolerant Routings in General Networks, with David Peleg, *Information and Computation*, 74, 1987, pp. 33-49.
- Pipeline Scheduling: a Survey, with Eugene Lawler, Jan Karel Lenstra, Charles Martel, and Larry Stockmeyer, IBM Research Report RJ 5738, 1987, San Jose, CA.
- Data Structures on Machines with Few Processors, with Friedhelm Meyer auf der Heide, IBM Research Report RJ 5240, 1986, San Jose, Ca.

- On Scheduling Unit-Time Jobs with Multiple Release Time/Deadline intervals, with Michael Sipser, *Operations Research*, 32, 1984, pp. 80-88.
- An Efficient Fault-Tolerant Algorithm for Clock Synchronization, with Joseph Halpern, Ray Strong, and Danny Dolev, *Proc. of the 1984 Principles of Distributed Computing*, Vancouver, British Columbia, 1984, pp. 89-102.
- Multiprocessor Scheduling of Unit-Time Jobs with Arbitrary Release Times and Deadlines, *SIAM J. on Comput.*, 12, 1983, pp. 294-299.
- On Scheduling with Release Times and Deadlines, *Deterministic and Stochastic Scheduling*, NATO Advanced Study Institutes Series, D. Reidel, Dordrecht, Holland, 1982.
- Minimizing Maximum Lateness for a Generalized Scheduling Model, IBM Research Report RJ 3237, 1982, San Jose, CA.
- Scheduling Unit-Time Tasks with Arbitrary Release Times and Deadlines, with Michael Garey, David Johnson, and Robert Tarjan, *SIAM J. on Comput.*, 10, 1981, pp. 256-269.
- A Fast Algorithm for Multiprocessor Scheduling, *Proc. Of 21st Annual Symposium on Foundations of Computer Science*, IEEE Computer Society, Syracuse, New York, 1980, pp. 50-53.
- On Minimum Circuits in a Graph, *Proc. of West Coast Conference on Graph Theory, Combinatorics, and Computing*, Humboldt State University, Arcata, California, 1980.
- A Fast Algorithm for Single Processor Scheduling, *Proc. of 19th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society, Long Beach, California, 1978, pp. 246-252.

Invited talks

- Invited Speaker, World Knowledge Forum, South Korea, Oct. 18-19, 2000.
- Invited Speaker, Distinguished Lecture Series, Ewha Women's University, South Korea, Oct. 2000.
- Invited Speaker, DIMACS Workshop on Management of Digital Intellectual Property, Rutgers Univ., April 17-18, 2000.
- Keynote Speaker, ACM Southeast Conference, Clemson Univ., April 6-7, 2000.
- Invited Speaker, Computers, Freedom, and Privacy Conference, Toronto, Canada, April 4-7, 2000.
- Keynote speaker, S. Africa, SAICSIT'99 (The South African Institute for Computer Scientists and Information Technologists), Johannesburg, South Africa, Nov. 17-19, 1999.
- Invited speaker, Distinguished Lecture Series in Information Science, Northeastern Univ., Oct. 25, 1999.
- Invited plenary speaker, ACM Special Interest Group on Computer-Human Interaction (SIGCHI), May 19, 1999.
- Invited plenary session speaker, 9th Annual Conference on Computers, Freedom, and Privacy, Washington, DC, April 1999.
- Invited speaker, Distinguished Lecture Series, Brown Univ., Feb. 14, 1999.
- Keynote Speaker, James E. Smith Midwest Conference on World Affairs, Univ. of Nebraska, Kearney, March 16-18, 1998.
- Invited speaker, Univ. of Maryland Distinguished Lecture Series, May 1, 1996.
- Invited Conference Chair and speaker, Intellectual Property, Patent and Copyright Protection on the Internet, Atlanta, GA, April 29, 1996.
- Keynote speaker, Computer Science Conference, Nashville, Tenn., Feb. 28, 1995.
- Invited lecturer, University Video Communications Distinguished Lecture Series, Aug. 26, 1994.
- Tutorial: Instruction Scheduling, with Vivek Sarkar, the IEEE/ACM Fifth Symposium on Parallel and Distributed Processing, Dec. 4, 1993, Dallas, Texas.

- **Invited speaker or panelist:**
  - Intertrust, Corp, Jan. 12, 2000.
  - Princeton, Univ., Dec. 7, 1999.
  - Univ. of Pennsylvania, Oct. 27, 1999.
  - "Beyond Computers", National Public Radio weekly program, Oct. 1999.
  - San Francisco Bay Chapter, ACM, Sept. 15, 1999.
  - ABA National Convention, Aug. 8, 1999.
  - Stanford Univ., April 20, 1999.

- U.S. Air Force Academy, March 3, 1999.
- New York Univ., Feb. 5, 1999.
- U. Mass. Amherst, Feb. 1, 1999.
- U.C. Berkeley, September 26, 1998.
- U.C. Davis, May 27, 1998.
- U.C. Santa Cruz, May 20, 1998.
- Purdue Univ., April 20, 1998.
- Dartmouth Univ., March 2, 1998.
- Univ. of Central Florida, Orlando, Florida, Sept. 29. 1997.
- "Intellectual Capital: Business Strategies, Legal Protections, and Global Competitiveness", Hoover Institution (Stanford), June 19, 1997.
- Univ. of California at Santa Barbara, April 21, 1997.
- Annual meeting of the ACM, San Jose, CA., March 2. 1997.
- National meeting of AAAS, Seattle, WA, Feb. 1997.
- WebNet-96, World Conference of the Web Society, San Francisco, Ca., Oct. 16-18, 1996.
- Computing Research Association Snowbird Conf., Snowbird, Utah, July 14-16, 1996.
- "Security and Freedom through Encryption Forum (SAFE)," Stanford Univ., July 1, 1996.
- IBM Almaden Research Lab, June 13, 1996.
- Univ. of Maryland, May 1, 1996.
- Stanford Univ., April 24, 1996.
- U.C. Berkeley, April 23, 1996.
- "The Future of Public Health: implications for Health Information/Communications Systems," sponsored by the Ca. Dept of Health Services and the Nat. Centers for Disease Control, San Diego, Ca., March 6, 1996.
- Feb. 17, 1996, ACM national meeting.
- "Policy Issues in the Development of Digital Media," ACM MULTIMEDIA'95, San Francisco, CA., Nov. 7, 1995.
- "The Good, the Bad, and the Internet," Chicago, Ill., Oct. 7, 1995
- DAGS '95 Conference on Electronic Publishing and the Information Superhighway, Boston, MA, June 1, 1995.
- "Issues in Science and Technology Policy," a Brookings Institute Conference for Corporate and Government Managers, Williamsburg, VA, May 21, 1995.
- National Public Radio's Science Friday, Feb. 17, 1995.
- IBM Boulder TechExpo series, Feb. 11, 1995.
- National meeting of AAAS, Atlanta, Ga., Feb. 1995.
- Workshop on Compiler and Architecture Issues for Future Generation Microprocessors: Superscalar, Superpipelined, VLIW and Hybrid., Toronto, Canada, Nov. 1, 1994.
- Networld/Interop Conference, Sept. 13, 1994.
- KPFA radio, Sept. 6, 1994.
- The Grace Hopper Celebration of Women in Computing, June 10, 1994.
- KQED radio, May 17, 1994.
- World Affairs Council, San Francisco, Ca., April 19, 1994.
- Computers, Freedom, and Privacy Conference, Chicago, March 24, 1994
- Conference on Information Technologies and their Implications, Carnegie-Mellon Univ., March 12-13, 1994.
- Lecture Series on Impact of New Information Technology: Multimedia and Networks, School of Library and Information Studies, U.C. Berkeley, Feb. 11, 1994.
- National meeting of the AAAS, San Francisco, Ca., Feb. 1994.
- National Public Radio's Science Friday, Dec. 10, 1993.
- EDUCOM national meeting, Oct. 18, 1993.
- Dagstuhl Seminar on Parallelizing Loops, Dagstuhl, Germany, June 17, 1993.
- Windows of Opportunity Symposium for Female Students in Computing, Washington, D.C., May 22, 1993.

- "Women Scientists and Engineers Employed in Industry: Why So Few?" Sponsored by the National Research Council, Jan 17-18, 1993.
- NASA Ames, Nov. 3, 1992.
- GMD at Carlsruhe, Germany, Sept 10, 1991.
- Sonoma State Univ. Math Colloquium, Oct. 30, 1991.
- U.C. Berkeley Engineering Alumni Society, Berkeley, CA, April 11, 1991.
- Eta Kappa Nu banquet, Berkeley, CA, Nov. 30, 1990.
- CPSR Annual Conference, Stanford Univ., Oct. 20, 1990.
- International Conference on Computing and Information, Niagara Falls, Canada, May 23-26, 1990.
- UCLA, Los Angeles, CA, May 8, 1990.
- TIMS/ORSA Conference, Vancouver, Canada, May 8, 1989.
- National meeting of the AAAS, San Francisco, Ca., Jan. 1989.
- Workshop on Parallel Compiler Optimization, Cornell Univ., 1988.
- International Conference on Foundations of Data Organization, Kyoto, Japan, May 22-24, 1985.
- TIMS/ORSA Conference, Dallas, Texas, Nov. 26-28, 1984.
- TIMS/ORSA Conference, San Francisco, Ca., May 14, 1984.

Policy Interactions with Government

- Invited Participant, the White House Conference on the New Economy, Washington, DC, April 6, 2000.
- Member, President's Export Council Subcommittee on Encryption, appointed 1998.
- Member, Information Technology Working Group of the President's Council on the Year 2000 Conversion, appointed 1998.
- Testified before the Commerce Committee of the California State Senate on encryption, Aug. 26, 1997.
- Testified at hearings before the National Committee on Vital and Health Statistics on privacy issues in the Kennedy-Kassenbaum Bill, San Francisco, CA, June 4, 1997.
- Testified in Social Security Administration hearing: Privacy and Customer Service in the Electronic Age, San Jose State Univ., May 28, 1997.
- Testified in hearing of the Subcommittee of Science, Technology, and Space of the Senate Committee on Commerce, Science, and Transportation on the "Pro-Code" Bill, S.1726, June 26, 1996.
- Testified on Intellectual Property and the Internet before a panel of the Mega-Project III of the Information Infrastructure Task Force (IITF) Advisory Council and the Security Issues Forum of the IITF, Sunnyvale, CA., Oct. 20, 1994.

Advisory Boards and Related Activities

- Berkeley Engineering Fund Board of Directors, U.C. Berkeley College of Engineering, starting 1998.
- Secretary, Council of Scientific Society Presidents, elected 1999. Elected to the Board of Directors, 1998.
- Member, steering committee, 21st Century Project. The 21st Century Project is a nationwide effort to reorient public support for research and development in science and technology toward solving some of the nation's most critical and basic problems.
- Advisory board, the Genome Radio Project and the Telecommunications Radio Project, the Science and Technology Radio Project, 1994 - 95.
- Corporate Affiliates and Advisory Board, Computer Science Division, U.C. Davis, 1991 - 1994.
- Dartmouth Institute for Advanced Graduate Studies, Dartmouth College, 1991 - 1995.
- Advisory committee, Excellence and Diversity Student Programs, Department of Electrical Engineering and Computer Science, U.C. Berkeley, 1989 - present.
- Member, advisory group, joint ACLU-CPSR project on a national ID card and privacy, 1989 - 91.
- Advisory committee, reentry program in computer science, U.C. Berkeley.
- Member, advisory committee at Mills College for program for returning adults.

ACM and Related Activities

- ACM President, 1998 - 2000.
- Founder and Chair, ACM Committee on U.S. Public Policy (USACM), 1993 – 1998
- Member, Computing Research Association (CRA) committee on Public Policy, 1992 - present.
- Secretary of ACM, 1990 - 92.
- Member, ACM Committee on Central and Eastern Europe 1990 - present.
- Vice-chair, SIGACT (Special Interest Group on Automata and Computability Theory of ACM) 1983-1990.
- Member, ACM Government Information Activities Committee, 1989 - 1990.
- Chair, ACM Committee on Scientific Freedom and Human Rights, June, 1987 - 1990.
- Chair, SIGACT Science Policy Committee, Nov. 1986 - 1990.

Other Professional Activities

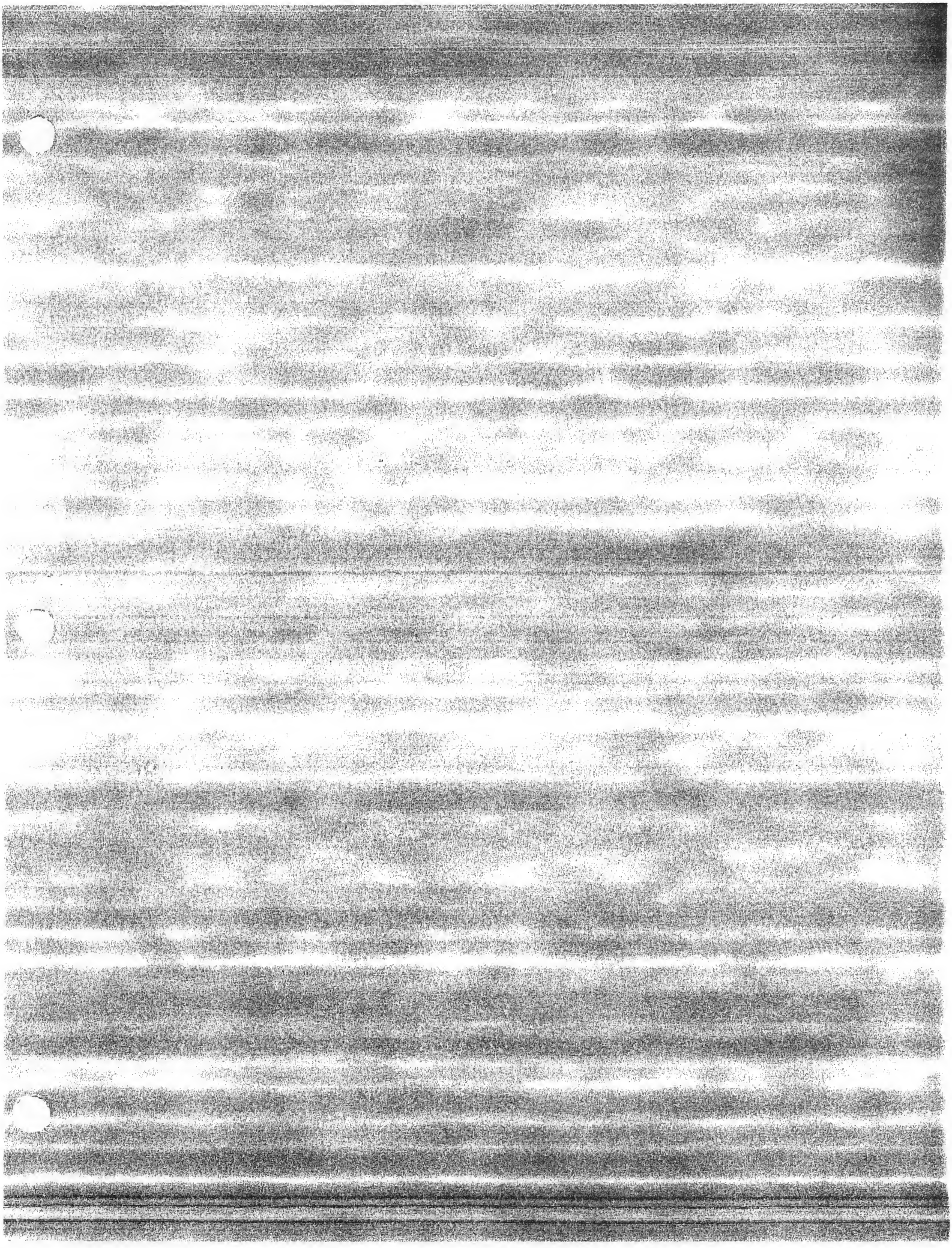
- Invited participant, Achieving XXcellence in Science (AXXS '99), Sponsored by the National Institutes of Health, Washington, DC, Dec. 9-10, 1999.
- Invited participant, National Academy of Engineering Summit on Women in Engineering, May 17-18, 1999.
- Invited participant, Women in Science Summit, The Women's Leadership Institute at Mills College, Sept. 29 - Oct. 1, 1994.
- Invited participant, Center for the Advancement of Public Policy multi-media CD-ROM project on Women in the Sciences, March 31, 1994.
- Member, the National Science Foundation's Collaboratives for Excellence in Teacher Preparation program review panel, Washington, D.C., Sept. 9-11, 1992.
- Associate Editor, Journal of Computing and Information (JCI).
- Member, the National Science Foundation's Research Initiation Awards panel, Washington, D.C., 1989.
- Invited participant in workshop on Science, Engineering and Ethics: State-of-the-Art, sponsored by the AAAS, Feb. 15-16, 1988, Boston, MA.
- Member of the National Research Council's Graduate Fellowship Evaluation Panel in Computer Science, Washington, D.C., 1985 - 1987.
- Invited panelist, Forsythe Panel, Stanford Univ., 1986 and 1989.
- Invited participant, Conference on Women and Computers, sponsored by MIT, Nov. 1984, and May 1985.

Program Committees and Session Chairs

- Member, program committee, CFP (Conference on Computers, Freedom, and Privacy) 1999, 1995, 1993.
- Member, program committee, Society and the Future of Computing, 1995.
- Member, program committee, DIAC-94 (Directions and Implications of Advanced Computing), DIAC-92.
- Member, program committee, the Grace Hopper Celebration of Women in Computing, June 9-11, 1994.
- Member, program committee, ICCI '92 (International Conference on Computing and Information), ICCI '91, and ICCI '90.
- Member, Program Committee of the 1991 IEEE Symposium on Parallel and Distributed Processing (SPDP).
- Cluster organizer (select session chairs) for scheduling theory, TIMS/ORSA conference, Vancouver, British Columbia, 1989.
- Chair, session on Bin-Packing and Scheduling, Fourth SIAM Conference.
- Chair and organizer, Asilomar Workshop on Fault Tolerant Distributed Computing, March 16-19, 1986, Asilomar, Ca.
- Local arrangements chair, ACM Symposium on Theory of Computing, 1982.

Other Organizing Activities

- Chair, Steering Committee of the Coalition for Science & Technology in a New Era, organized at end of Cold War. Conceived of and co-organized the Coalition. Scientific and engineering societies represented at the initial meeting had a combined membership of well over a million people.
- Organizer and Project advisor, Funding Policy in Computer Science, 1986 - 91.
- Organizer and moderator of panels on funding issues held at the national meeting of AAAS (1989), ACM Symposium on Theory of Computing (1987), and the International Congress of Mathematicians (1986).
- Organizer, "SDI: How feasible? How useful? How robust?" a debate on the SDI, Dec. 19, 1985, Stanford Univ., Stanford, Ca.
- Co-organizer, Reentry Program in Computer Science at U.C. Berkeley.



Barbara Simons

To DVD or Not to DVD

The current legal DVD battle between the movie industry and the free/open software communities over DVD is a microcosm of an ongoing intellectual property war. This war pits intellectual property owners against such diverse groups as programmers opposing restrictions on reverse engineering and the publication of computer code and librarians opposing new restrictions on copyright rights of first sale and fair use.

Jon Johansen may be the youngest victim of this war. Because of software posted on the 16-year-old's Web site, his home in Norway was raided in January by police who seized two computers and a cell phone. Both Jon and his father were indicted; criminal charges could result in two- to three-year prison sentences.

The software published by Johansen, called DeCSS, decrypts Content Scrambling System (CSS), the encryption software for DVD movie discs. Although much of the news coverage claimed that Johansen had broken CSS in a few hours, it appears that CSS was broken by others, most of whom posted their results anonymously. One of the reasons that the myth of Johansen's breaking CSS took hold is that CSS is amazingly weak. CSS uses only a 40-bit key, a length known to be breakable in a few minutes by exhaustive search. It also employs a proprietary algorithm, rather than one extensively tested in the public domain. The copy protection system relies heavily on obfuscation which, together with the carelessness of one licensee, appears to have created additional opportunities to break the system.

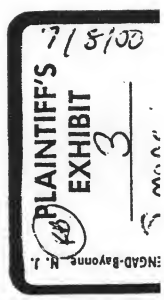
Concerns about the vulnerability of their protection scheme was a motivating factor for extensive lobbying by Hollywood and the DVD manufacturers on behalf of the anti-infringement component of the Digital Millenium Copyright Act (DMCA), passed in 1998. Quoting from *Emedia Professional* in 1997, "The film industry has submitted 'Anti-Circumvention' legislation to Congress in order to criminalize products or actions that would bypass the copy protection system" [1]. An earlier article in the *Electronic Engineering Times* stated "Also unresolved ... on the policy side [is] the language of a draft for anti-circumvention legislation. That proposed law must be agreed upon by movie studios, computer and consumer companies"[2].

Authentication, which verifies that a player or operating system has been licensed, is used to protect the proprietary algorithm and to discourage the manufacture of non-compliant DVD players. The DVD Copy Control Association (DVD CCA) was created in December 1999 to issue licenses. To obtain a license, a fee is paid and an agreement is signed pledging not to produce non-compliant machines or to reveal the copy protection scheme. The Linux community was divided. One group, LSDVD, has been working on a licensed DVD player; another, LiViD, was working on creating a free open-source version of DVD for Linux. Because there is no one who can speak for the entire community, a clash with the open/free software community was preordained, if not actually intended.

Johansen is not the only person facing legal proceedings. As of this writing there are three lawsuits—in California, New York, and Connecticut. Preliminary injunctions have been issued in California and New York, where plaintiffs also attempted to obtain preliminary injunctions against Web sites that link to others containing the DeCSS code. The California judge refused to grant Web site injunctions; there is still the possibility of the granting of such injunctions in New York.

The New York and Connecticut cases, brought by the eight largest movie studios, is based on the DMCA's prohibition on the circumvention of "copyright management information." (For a discussion of the possible negative impact on computer security R&D of the DMCA, see "Outlawing Technology," *Communications*, Oct. 1998, p. 17). The California case, brought by the DVD CCA, is based on misappropriation of trade secrets. While the defendants never signed a nondisclosure agreement, DVD shrink-wrap licenses forbid reverse engineering. (See

MARTIN MAYO



• From the President

"Melissa's Message," *Communications*, June 1999, p. 25; it discusses UCITA, an on-going attempt to legalize some of the most egregious aspects of shrink-wrap licenses). If you wish to obtain a copy of the DeCSS source code, the DVD CCA thoughtfully provided it in the California case (cryptome.org/dvd-hoy-reply.htm#Exhibit B). Or you can wear it on a T-shirt (to order, go to copyleft.net/cgi-bin/copyleft/t039.pl?1&back).

Many of those involved with breaking CSS say they did so to make it possible to play legally purchased DVDs on Linux and other free/open-source-based operating systems. Although the DMCA outlaws almost all reverse engineering of copy protection systems, reverse engineering for compatibility is specifically not prohibited by the DMCA; so the compatibility issue could become an important point in the New York case.

None of the defendants is accused of making illegal copies of DVDs—only of providing software that makes it possible to play a DVD disc on any computer with a DVD drive. Nor is DeCSS a prerequisite for making illegal copies. The main function for CSS appears to be to protect a monopoly on licensing the player market and to inhibit the widespread production of illegal DVDs and non-compliant machines.

What would have happened had the DVD CCA licensed all Linux and other free/open-source operating systems, or eliminated the licensing requirement altogether? Surely the risk of illegal copying of DVDs would not be any greater than it is now, with DeCSS widely available. Given the weaknesses of the DVD copy protection system, it seems likely that others would have broken CSS. Would their case have been significantly impaired because they couldn't argue that the reverse engineering was legal under the DMCA for reasons of compatibility? Or would the courts eventually have determined, as in the Bernstein case, that code is a form of speech and thereby protected in the U.S. under the First Amendment?

The consortium that imposed the DMCA on the country confronted a difficult problem. Was the DVD group's goal of preventing wholesale illegal copying a reasonable goal? Could a robust solution for protecting DVD's have been developed, or would any attempt, even one using strong encryption, have been doomed to failure? Did the DVD group make a fundamental mistake by failing to modify its business model to be more compatible with the new distribution environment?

ACM also has dealt with problems related to the ease of copying digitized material. The success of its digital library, even though copyright policy allows unlimited noncommercial copying, demonstrates that it's possible to remain financially solvent without resorting to draconian measures such as those contained in the DMCA. Is there a way that the ACM model or something similar could be applied to the movie industry? Or are the financial demands of a for-profit business simply too great to be compared to those of a not-for-profit?

Perhaps 20 years from now people will look back in amazement at our lack of understanding and insight. But this thought is of little comfort either to those who are being threatened with large fines and prison sentences or to intellectual property owners who fear wholesale illegal copying.

We knew bad legislation posed risks to free speech and standard procedures such as reverse engineering. Unfortunately, we now have moved from the theoretical to a concrete demonstration. Unless the most insidious portions of the DMCA are repealed or declared unconstitutional and UCITA is stopped, there will be damage to legitimate and accepted practices for the advancement of computing, to say nothing of significant restrictions on even more basic rights.

We need to declare a truce in the intellectual property war and start a discussion about how intellectual property owners can receive fair compensation without resorting to restrictions on technology and speech. ■

References

1. Hughes, K. DVD video encryption update: Hollywood, having cake and eating it. *Emedia Professional 10*, 6 (Jun. 1997) 54–59.
2. Yoshida, J. Intel weighs in on DVD encryption. *E. Eng. Times* (Oct. 14, 1996), 923, 1,142.

BARBARA SIMONS (simons@acm.org) is ACM's president and welcomes your feedback.

© 2000 ACM 0002-0782/00/0500 $5.00